

管理画面の見覚えのない 管理者アカウントに関する調査報告

対象	サンプル商店（架空）のEC-CUBE 4系のサイト。管理画面、EC-CUBEの記録（ログ）、サイトのファイル
報告	クマひよ工房

この見本は、架空のサイトをもとにしたものです。実際のご報告も、この並びでお渡しします。

1. まとめ

わかったこと	見覚えのない管理者アカウントは、以前の担当の方のアカウントで管理画面にログインした誰かが作ったものでした。
わからなかったこと	以前の担当の方のパスワードが、どこから知られたのかは特定できませんでした（理由は「4. 調べた範囲と、調べられなかった範囲」）。
主な影響	作られたアカウントで、受注の一覧が閲覧された記録があります。お客様の個人情報が見られた可能性があります。
対応の方針	クマひよ工房でできる対策をすぐに進めるとともに、見られた情報の範囲を確かめるため、セキュリティの専門会社へのご相談をおすすめします。

2. 何が起きたのか

管理画面に、作った覚えのない管理者アカウントがありました。

記録を順にたどると、次のことが分かりました。

1. 以前の担当の方のアカウントで、普段とは違うアクセス元から管理画面にログインがあった
2. その直後に、見覚えのない管理者アカウントが作られた
3. 作られたアカウントで、受注の一覧が開かれた

たとえるなら…

お店の合鍵を持ったまま辞めた方の鍵が、知らない誰かの手に渡り、その鍵で入った人が、自分用の合鍵をもう1本作っていた状態です。

3. 影響の範囲

起きた可能性があること	受注の一覧に表示される、お客様のお名前、ご住所、ご注文の内容が見られた可能性があります。
今回の調査では見つからなかったこと	サイトのファイルの書き換え、商品や価格の変更、ほかの管理者アカウントの作成。ただし、見つからなかったことは、起きていないことの証明にはなりません。
業務への影響	今のところ、注文の受付や決済は、いつもどおり動いています。

4. 調べた範囲と、調べられなかった範囲

調べた範囲	調べられなかった範囲
管理画面のアカウントの一覧と、作られた日時	サーバのアクセスの記録（ご契約のレンタルサーバでは見られないため）
EC-CUBEの記録（ログ）のうち、残っていた期間のもの	残っていた期間より前の記録
サイトのファイルと、EC-CUBEの配布元のファイルとの比べ合わせ	以前の担当の方がお使いのパソコンや、メール

5. うまく働いていた点

EC-CUBEの記録（ログ）が残っていたため、アカウントが作られた経路をたどれました。

6. 対策のご提案

順	対策	内容と効果	お客様への影響
1	見覚えのないアカウントの停止（ご了承のうえ実施済み）	これ以上使われないようにしました。調査の手がかりを残すため、削除はしていません。	なし
2	すべての管理者のパスワードの変更	知られている可能性のあるパスワードを使えなくします。	管理画面をお使いの方に、新しいパスワードをお伝えする手間がかかります
3	使っていないアカウントの整理	辞めた方のアカウントを残さないようにします。	なし
4	管理画面のログインを強める	ログインの失敗が続いたアカウントを止める、ログインできるアクセス元を絞るなどで、同じ入られ方を防ぎます。	ログインの手順が少し変わる場合があります

対策2～4のお見積りは、別紙のとおりです。

7. 専門会社へのご相談について

判定

専門会社へのご相談をおすすめします。

理由

- お客様の個人情報が見られた可能性があり、その範囲を確かめる必要があるため
- サーバのアクセスの記録を見られず、クマひよ工房の調査では追いきれないため

クマひよ工房でお手伝いできること

専門会社にご依頼される場合は、今回調べた記録やソースコードのご提供、サイトの構成のご説明、専門会社が提案した対策の実装をお手伝いします。